情報防護クラウドセキュリティ プラットフォーム

People-Centricアプローチに基づくアクセス制御、脅威対策、内部脅威対策、データセキュリティでハイブリッド クラウドを保護

製品

- Proofpoint CASB (Cloud App Security Broker)
- Proofpoint Web Security
- Proofpoint ZTNA (Zero Trust Network Access)
- Proofpoint ITM (Insider Threat Management)
- Proofpoint Endpoint DLP (Data Loss Prevention)
- Proofpoint Email DLP (Data Loss Prevention)

主なメリット

- 管理と対応の両方が可能なクラウドネイティブなプラットフォーム
- メール、クラウド、Web、エンドポイントに対してPeople-Centricな可視性と制御を実現
- ワールドクラスの脅威、コンテンツ、振る舞い分析と高度な分析ツール
- 共通のデータ分類子とメール、クラウドアプリ、Web、エンドポイントに対するコンテンツ スキャン
- SASE対応のセキュリティ アーキテクチャと柔軟なデプロイモデル

セキュリティにおいてネットワーク境界の概念はなくなりました。その代わりに境界となったのは「人」です。テレワークが普及し、個人所有のデバイスと管理されていないアプリが仕事で使用されています。インフラやデータをパブリッククラウドに移行する企業も増えています。人を狙ったサイバー攻撃はこれまで以上に増加しています。こうした環境においてクラウドとデータを保護するには、「人」を中心としてセキュリティを構築する必要があります。

ユーザーは、Web、クラウドサービス、プライベートアプリに安全にアクセスしなければなりませんが、1つのソリューションだけで、この安全なアクセスを実現することはできません。アクセス制御、脅威対策、データセキュリティ、アプリのガバナンス、ゼロトラスト ポリシー制御などのソリューションを組み合わせて使用することが重要です。ユーザーとデータのアクティビティをエンドポイント全体で保護するには、すべてのチャネルにセンサーを導入し、制御を行う必要があります。また、分析、調査、ポリシー管理を行う共通のプラットフォームを用意しなければなりません。

この課題を解決できるのがプルーフポイントの情報防護クラウドセキュリティ プラットフォームです。このプラットフォームでは、多くの製品を組み合わせて、セキュアアクセス、データ損失防止（DLP）、内部脅威対策を行います。また、ワールドクラスの検知機能で、脅威、コンテンツ、動作を分析します。このプラットフォームは、「人」を基点としてセキュリティを構築するPeople-Centricの観点から可視性を実現し、Web、クラウド、プライベートアプリに対するアクセスを制御します。統合されたコンソールで、管理作業と脅威対応を行うことができます。また、高度な分析結果が提供されるため、作業を省力化し、対処時間を短縮できます。

プルーフポイントの情報防護クラウドセキュリティ プラットフォームは強力でクラウドネイティブなプラットフォームです。また、セキュアサービスエッジ（SSE）アーキテクチャという業界のビジョンにも対応しています。SSEは、ユーザーの場所や使用するデバイスに関係なく、人がアプリやデータにアクセスするときにセキュアアクセスを提供し、脅威から保護します。プルーフポイントのプラットフォームが収集するデータはアップロードするリージョンを端末毎に選択し、保存出来ます。これにより、どこで作業を行っても、地域固有のデータ コンプライアンス要件を提供できます。また保存したログはグローバルで統合管理することも可能です。

このプラットフォームで使用する製品は次のとおりです。

- Proofpoint Enterprise DLP
- Proofpoint CASB (Cloud App Security Broker)
- Proofpoint Email DLP and Proofpoint Email Encryption
- Proofpoint ITM (Insider Threat Management) と Proofpoint Endpoint DLP
- Proofpoint Web Security と Proofpoint Browser Isolation
- Proofpoint ZTNA (Zero Trust Network Access)

脅威を阻止して、クラウド、Web、プライベート アプリにセキュアアクセスを提供

プルーフポイントのクラウドセキュリティはグローバル規模で、クラウド ネイティブなプラットフォームです。People-Centric アプローチに基づいたアクセス制御と脅威対策、ゼロトラスト ネットワークなどから構成されます。このプラットフォームでは、次のものを組み合わせて、クラウド サービス、Web プライベートアプリを保護します。

- **きめ細かい制御:** 認証の設定、ブラウザ分離による読み取り専用アクセス、マイクロセグメント化されたアプリのアクセスなどを行います。
- **豊富な脅威インテリジェンス:** ユーザーのリスクに対して、製品間で豊富な脅威インテリジェンスが連携されます。
- **高度な脅威対策:** 侵害されたアカウントと不正なOAuthアプリを検知し、修復します。また、マルウェアも阻止します。リスクの変化を検知するため、ユーザーとエンティティの振る舞い分析（UEBA）も組み込まれています。
- **インラインかつリアルタイムに動作するDLP:** クラウド上の機密データへの不正アクセスを阻止し、対応を継続します。
- **可視性:** シャドウIT、SaaS用クラウドアプリのガバナンス、サードパーティのOAuthアプリ、IaaS（Infrastructure as a Service）サービスのインフラとしてのクラウド セキュリティ情報を監視します。
- **マルチモードアーキテクチャ:** 可視性とアダプティブ コントロールを実装します。

プルーフポイントのプラットフォームでは、リスクの高いユーザーに対して、より厳密な制御を行うことができます。これらのユーザーは脆弱であったり、攻撃の標的になりやすい人物です。adminやVIPなどの特権グループのメンバーにすることもできます。

重要なチャネルでの機密データの保護と内部脅威リスクの管理

プルーフポイントの情報防護は、クラウド上の機密データを検出し、データの漏洩を防止します。このソリューションは、メール、クラウドアプリ、Web、エンドポイントで機能します。共通のデータ分類子、ディテクター、タグ付けのフレームワークを使用して、エンタープライズ全体で整合性のあるポリシーを設定できます。これらのチャネルのコンテンツ、行動、脅威テレメトリーを統合し、DLP アラートの原因となったユーザーが、侵害の結果なりすまされているのか、悪意を持っておこなっている行為なのか、または不注意でおこなった行為なのかを迅速に把握できます。また、これらのチャネルでDLPアラートが一元管理されるため、優先度の高いアラートに迅速に対応することができます。

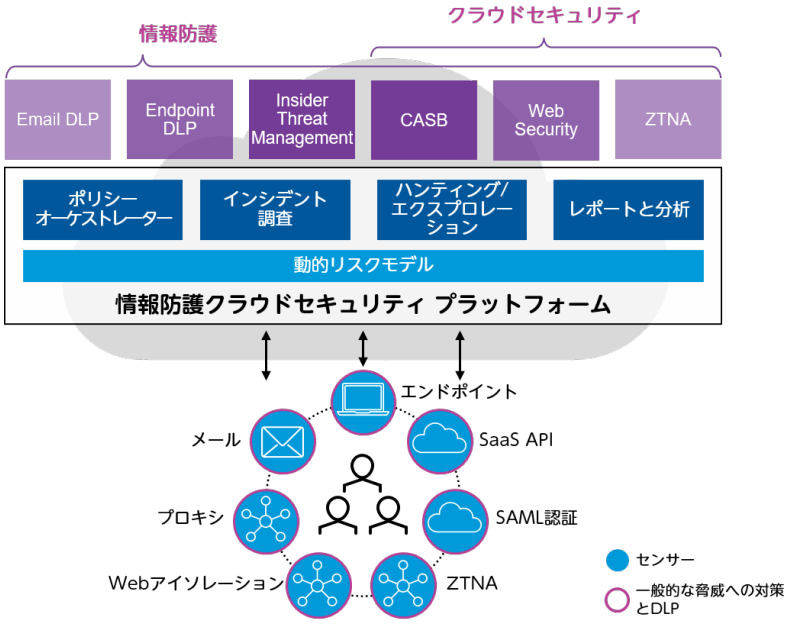

図1: プルーフポイントの情報防護クラウドセキュリティ プラットフォーム

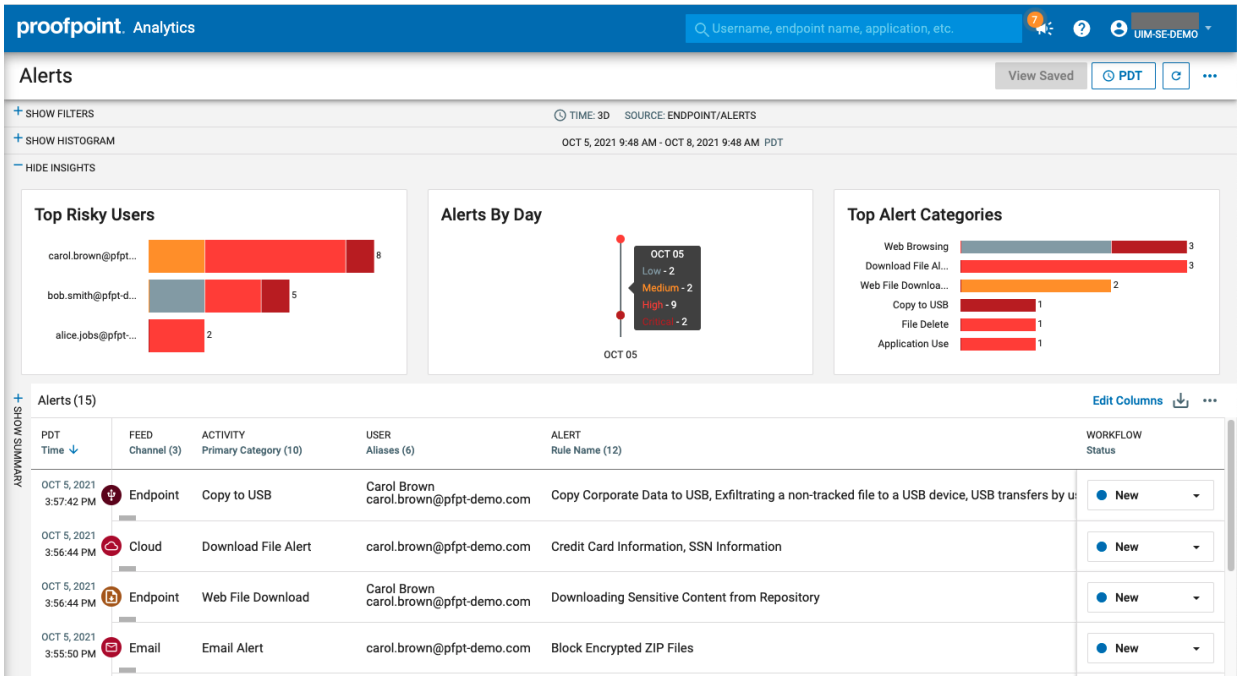

図2: 統合されたコンソールで管理作業と脅威対応を実施

内部脅威リスクとエンドポイントでのデータ損失は互いに結びついています。プルーフポイントのプラットフォームを使用すると、セキュリティチームはリスクの高いユーザーに優先的に対応し、内部脅威リスクを検出して、脅威に迅速に対処することができます。また、ユーザーのアクティビティをきめ細かく、リアルタイムで可視化できます。データ損失チャネルでは、データ損失と内部脅威リスクのアラートが統合されています。これにより、イベントとアラートに関連する人物、対象、場所、時間、理由を迅速に確認できます。

高度な分析ツールを備えた統合コンソール

プルーフポイントの統合コンソールでは、管理作業とリスク対応を行うことができます。次のツールを使用して、効率的に調査作業を進めることができます。

- ポリシー管理
- インシデントと調査のワークフロー
- 脅威ハンティングとエクスプロレーション
- レポートと分析
- 管理とデータプライバシー

ポリシー管理

このプラットフォームでは、次のことが可能です。

- 1つのコンソールで、クラウドとデータに対するすべてのアクセスポリシーを管理する。
- 次のものを使用して、複数のチャネルに高度なルールを作成する。
  - 共通のデータ分類子（スマートID、辞書）
  - ディテクター（近接マッチング）
  - ディテクターセット（ユーザーグループ、リージョン、ユースケース、チャネル）
  - 機密性ラベル
  - 高度な脅威インテリジェンスと検知

インシデントと調査のワークフロー

このプラットフォームでは、次のことが可能です。

- 脅威、DLP、ユーザーの振る舞いに関するアラートを収集して、アラートマネージャーに統合する。これにより、ユーザーの全体的なリスクプロファイルを作成可能。
- 各セキュリティイベントに関連する人物、対象、場所、時間、理由を常に確認する。
- ユーザーの振る舞いを調査し、意図とリスクの重大度を判断する。
- 検出から解決まで、部門間でアラートステータスを管理する。

脅威ハンティングとエクスプロレーション

このプラットフォームでは、次のことが可能です。

- 新しい脅威に対するプロアクティブなハンティングを実施し、クラウドアカウントの侵害、データの持ち出し、データの漏洩、内部脅威リスク、未承認アプリの使用などの脅威を調査する。
- ウォッチリストを作成して、経営陣、Very Attacked People™（VAP）、部門ユーザー、特権ユーザー、人事部スタッフ、契約業者などのリスクプロファイル別にユーザーをまとめ、優先順位を設定する。人事ウォッチリストからウォッチリストを作成することも可能。
- 検索機能と強力なフィルターを使用して、すぐに使えるようにエクスプロレーションをカスタマイズする。

レポートと分析

このプラットフォームでは、次のことが可能です。

- 分かりやすいタイムラインベースのビューで、複数のチャネルのユーザーとデータのアクティビティを確認する。
- ユーザーの意図に基づくリスク アクティビティのレポートをビジネスパートナーと共有する。
- 他のセキュリティツールから取得したデータを使用して、複数のチャネルのアクティビティとアラートを相関分析する。これは、SIEM（セキュリティ情報/イベント管理）、SOAR（セキュリティ オーケストレーション、自動化、対応）、チケッティングシステムのシームレスな統合で実現されている。

管理とデータプライバシー

このプラットフォームでは、次のことが可能です。

- 役割ベースのアクセス制御を使用して、アラートと調査結果を部門間で管理する。
- きめ細かい、属性ベースのアクセス制御を使用して、データプライバシーの問題に対応する。
- 組織のシングル サインオン（SSO）プロバイダー（Microsoft、Okta Identity Cloud、Google Cloud IAMなど）を使用して、OAuth経由でプラットフォーム ユーザーの認証を行う。

製品

プルーフポイントの情報防護クラウドセキュリティ プラットフォームでは、Proofpoint CASB、Proofpoint Email DLP、Proofpoint ITM と Proofpoint Endpoint DLP、Proofpoint Web Security と Proofpoint Browser Isolation、Proofpoint ZTNAが統合されています。このセクションでは、各製品について説明します。

Proofpoint CASB

Proofpoint CASBは、クラウドアカウントの検出、DLP、サードパーティ アプリのガバナンスをPeople-Centricなコントロールで統合しています。これにより、Microsoft 365、Google Workspace、Box、Salesforce、AWS、Azure、Slackなどに安全にアクセスすることができます。プルーフポイントのマルチモードCASBは、APIとプロキシベースの両方のデプロイモデルに対応しています。

Proofpoint Email DLP

Proofpoint Email DLPは、メール経由でのデータ侵害のリスクを軽減します。240を超える組み込みの分類子を使用して、PCI、PII、PHI、GDPRの要件を満たします。単体のソリューションよりも簡単かつ低価格で、可視化と適用を行うことができます。

Proofpoint ITMと Proofpoint Endpoint DLP

Proofpoint ITMとProofpoint Endpoint DLPは、内部関係者によるデータ損失ブランド価値の毀損を防ぎます。USB、クラウド上の同期フォルダー、印刷などによるデータの持ち出しを阻止します。これらの製品は、権限のあるユーザーの悪意や怠慢による被害から組織を保護します。エンドポイントベースでデータの操作を完全に可視化します。内部関係者によるデータ侵害から守り、インシデント対応を迅速に行うため、ユーザーのアクティビティとデータの移動を関連付けて分析します。

Proofpoint Web Securityと Proofpoint Browser Isolation

Proofpoint Web Securityは、Webを閲覧する従業員を高度な脅威から保護します。巧妙なサイバー脅威だけでなく、データの損失も防ぎます。People-Centricアプローチに基づき、ポリシーを使用してリスクを軽減します。Proofpoint Web Securityは、動的なアクセス制御、高度な脅威対策、DLPポリシーを提供します。この製品は、プルーフポイントの業界最高クラスの脅威インテリジェンスとNexus Threat Graphを使用します。Proofpoint Web Securityはクラウドネイティブなソリューションです。きめ細かい制御を行い、未知のサイト、不審なサイト、Webメールなどの個人使用のサイトをアイソレーションし分離環境で実行します。

Proofpoint ZTNA

Proofpoint ZTNAは、VPNに代わるゼロトラストのソリューションです。ユーザーの場所に関係なく、エンタープライズアプリへのリモートアクセスを保護します。プルーフポイントのPeople-Centricソリューションにより、数多くのクラウドインスタンスに対して、マイクロセグメンテーションによるセキュアなアクセスを提供します。また、クラウド間の接続を自動化することもできます。オンプレミス サーバーとパブリッククラウド間でハイブリッドなクラウド ネットワークを実現できます。

詳細

詳細は**proofpoint.com/jp**でご確認ください。